Hindawi Publishing Corporation
Journal of Sensors
Volume 2015, Article ID 469793, 10 pages
http://dx.doi.org/10.1155/2015/469793

Research Article

ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks

Pu Gong,[1,2] Thomas M. Chen,[2] and Quan Xu[2]

[1]*Key Lab of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[2]*Department of Electrical and Electronics Engineering, City University London, London EC1V 0HB, UK*

Correspondence should be addressed to Pu Gong; pu.gong.1@city.ac.uk

Received 31 October 2014; Accepted 25 December 2014

Academic Editor: Fanli Meng

This paper presents a new routing protocol called Secure and Energy Aware Routing Protocol (ETARP) designed for energy efficiency and security for wireless sensor networks (WSNs). ETARP attempts to deal with WSN applications operating in extreme environments such as the battlefield. The key part of the routing protocol is route selection based on utility theory. The concept of utility is a novel approach to simultaneously factor energy efficiency and trustworthiness of routes in the routing protocol. ETARP discovers and selects routes on the basis of maximum utility with incurring additional cost in overhead compared to the common AODV (Ad Hoc On Demand Distance Vector) routing protocol. Simulation results show that, in comparison to previously proposed routing protocols, namely, AODV-EHA and LTB-AODV (Light-Weight Trust-Based Routing Protocol), the proposed ETARP can keep the same security level while achieving more energy efficiency for data packet delivery.

1. Introduction

Ad hoc networks are self-configuring wireless networks of mobile devices without a fixed infrastructure, and wireless sensor networks (WSNs) are a type of ad hoc networks consisting of wirelessly interconnected sensor nodes. Sensor nodes may have functions including sensing, data relaying, and data exchanging with other networks outside the WSN [1]. WSNs may range in size from a few to hundreds of thousands of nodes.

While WSNs are useful for a wide variety of applications, this paper is focused on applications operating in extreme environments such as the battlefield where the risk of harm prohibits any manual engineering work. Various WSN applications can be deployed in the battlefield. For soldier detection and tracking (SDT), unattended acoustic and seismic sensors are deployed at specific points to detect the approach of enemy soldiers in order to protect military sites or buildings [2]. Sensors can detect typical sounds made by soldier activities, for example, walking, crawling, weapon handling, and talking, at a distance. Another example of interest here is littoral antisubmarine warfare (ASW) that utilizes small and low cost sensors equipped with passive or active sonar, which can be deployed in large numbers (hundreds or thousands) to provide a high density sensor field to detect enemy submarines [3]. These sensors have a short detection range and are far less susceptible to multipath reverberations and other acoustic artifacts.

There are many other WSN applications that share certain features with these two examples. First, nodes are usually deployed without careful preplanning (e.g., airdrop deployment) since the battlefield is a dangerous zone, and sending engineers to carry out precise deployment is not preferable. Thus network topology is not known a priori and will likely change over time due to exterior forces (e.g., explosions and movements). The networks are ad hoc by necessity in these environments.

Second, the nodes in the applications of interest are often physically unreachable after deployment. Consequently, replacement of the energy source (typically battery) is difficult or impossible. In order for the network to operate as long as possible, nodes may be capable of harvesting energy, and network routing protocols should select routes to minimize energy cost.

Third, the network faces the risk of attacks to interfere with operations, such as selective forwarding, wormhole

attacks, sinkhole attacks, and Sybil attacks [4]. Nodes may become compromised which could be very difficult to detect. It is commonly assumed that compromised nodes may exhibit suspicious behavior, which is monitored and factored into a reputation system that calculates a reputation for every node and adapts route selections to avoid nodes with low reputations. Moreover, suspected nodes are prevented from participating in the routing protocol.

While routing protocols have been proposed for energy efficiency or security separately, the new routing protocol proposed here balances the two objectives simultaneously by means of utility theory. To the best of our knowledge, this is an original approach for WSN routing protocols. An essential component of the routing protocol is a new method to estimate energy consumption for packet forwarding. Another essential element is a Bayesian network to judge the probability of each node being compromised (or introduce a reputation or trust).

The contributions of this paper are as follows. First, a novel energy efficient routing protocol is proposed which aims to minimize energy consumption for data transmission. The second contribution is the novel use of utility theory to simultaneously consider two factors: energy efficiency and trustworthiness of nodes. Third, a Bayesian network is used to estimate the trustworthiness of nodes which is a different approach from previous literature.

Section 2 is a review of related work. In Section 3, the central concepts in the new Energy Efficient Trust-Aware Routing Protocol (ETARP) are presented. The methods to estimate energy consumption and risk of node compromise are explained. Performance evaluation in terms of simulation results is presented in Section 4. Section 5 concludes the paper.

2. Related Work

Many routing protocols have been proposed for WSNs; for instance, see a good survey by Royer and Toh [5]. These traditional routing options for WSNs include the data centric approach such as Directed Diffusion and reactive approach such as Dynamic Source Routing (DSR). Particularly, a reactive approach called Ad Hoc On-Demand Distance Vector (AODV) routing has been a popular candidate due to advantages in coping with the ad hoc nature of some WSNs as AODV does not require knowledge of the global network topology.

Some efforts have been made to improve the energy efficiency of the routing protocol itself. For example, the routing method described in [6] attempted to minimize the energy consumed for routing data packets, but the drawback is that location information is required. In [7], the author provides a simple, scalable, and efficient solution for minimum cost routing in WSNs. In fact, the term "minimum cost" refers to maximum network lifetime, achieved by choosing the route with maximum energy reserve which is not exactly the same as a route with minimum energy cost. Another approach of minimum cost message delivery was studied in [8]. This approach sought the minimum cost path from any given source to a specific sink in sensor networks. This approach may not be suitable for some WSN applications because the sink (or destination node) is assumed to be fixed.

2.1. Energy Harvesting Aware Routing Protocols. Another research direction considers renewable energy from an external energy source. Renewable energy can be harvested from the surrounding environment by various means such as solar, wind, thermal, or motion [9]. Solar power is well suited to WSNs because not only sunlight is easy to access but also solar panels can be made small enough to be mounted on wireless sensor nodes.

A notable routing algorithm that is energy harvesting aware is the Distributed Energy Harvesting Aware Routing Algorithm (DEHAR) [10], which defines a new metric of "energy distance" (including energy harvesting) for selecting the best route. By this metric, DEHAR aims to find the route with minimum total energy distance rather than spatial distance. But DEHAR calculates the shortest energy distance by using a method such as directed diffusion, a flooding mechanism incurring extra routing overhead. In contrast, ETARP proposed here avoids extra overhead in route discovery (compared to AODV). OR-AHaD (Opportunistic Routing algorithm with Adaptive Harvesting-aware Duty Cycling) proposed in [11] is designed with energy management capabilities that consider variations in the availability of the environmental energy. OR-AHaD can adjust the duty cycle of each node adaptively in order to exploit the available energy resources efficiently in comparison to other opportunistic routing protocols. But geographical information is required, which is not well suited to the applications of interest here.

2.2. Secure Routing Protocols. Security challenges in WSNs are similar to those in mobile ad hoc networks identified in [12, 13], and some existing routing protocols such as TinySec [14], Spins [15], TinyPK [16], and TinyECC [17] attempt to eliminate unauthorized behavior of malicious sensor nodes with the help of encryption or authentication on data packets. However, these solutions may be difficult for WSNs. For instance, data encryption is applicable for mobile ad hoc networks but generally not practical for WSNs because sensors have limited data processing capabilities and energy storage.

In addition to cryptographic solutions, routing algorithms that employ notions of trust and reputation have been proposed, such as trust-based on-demand multipath routing (AOTDV) [18] and light-weight trust-based routing protocol (LTB-AODV) [19]. They passively observe forwarded data traffic and then calculate the risk level of different routes in terms of "trust values." The routing algorithm then chooses the most trusted route. Compared to ETARP, the reputation system used in AOTDV or LTB-AODV watches for a single specific behavior only, not like the Bayesian network adopted in ETARP. ETARP monitors multiple node behaviors and makes comprehensive judgments on node status. Furthermore, AOTDV or LTB-AODV focuses only on security with no special attention given to energy efficiency concerns.

2.3. Routing Protocols including Energy Harvesting and Security. There are a few papers starting to consider security and energy efficiency at the same time. For instance, Ferng and Rachmarini [20] proposed a secure routing protocol for WSNs considering energy efficiency, but compared to ETARP, it has a disadvantage requiring information about node locations to improve energy efficiency. Furthermore, it depends on encryption which can be a heavy computation cost for sensor nodes. LS-LEACH [21] is another energy aware routing protocol, based on the LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol, that depends on cryptographic authentication. The scheme generates extra overhead compared to ETARP.

3. ETARP Routing

This section describes the ETARP routing protocol designed for the WSN applications mentioned in Section 1. The routing protocol aims to simultaneously consider energy efficiency and security to avoid routes that are inefficient and risky. In order to simplify the description, we assume for the moment a "normal" condition absent of attacks in the network. In this case, ETARP works to discover and select the most energy efficient routes. In the next section, attacks on the network will be taken into account to show how ETARP factors trustworthiness of nodes into the route selection. Because energy efficiency and security are two different problems, ETARP takes a novel approach of factoring both using the notion of expected utility.

A basic example to demonstrate the idea of ETARP is shown in Figure 1. After the enemy appears in the WSN covered region, their activity can be detected by a nearby sensor node (e.g., acoustic or seismic sensor) which will send warning information back to the data collection point. Usually this process cannot be accomplished in a single hop transmission; ETARP serves to find the most energy efficient multihop route while simultaneously avoiding any (perceived) compromised nodes. The status of nodes is estimated by a Bayesian network that collects data about observed node behaviors and calculates the probability that each node is compromised or not.

3.1. Energy Efficiency Routing in Absence of Attacks. For the moment, attacks on the network are ignored to present how ETARP operates to discover and select energy efficient routes. Previous studies have found that the ad hoc nature of the network dictates an on-demand routing protocol such as AODV. However, AODV aims to minimize hop count without consideration of energy costs. ETARP is based on AODV but adds awareness of transmission energy costs.

The route discovery by ETARP operates similarly to AODV except for a different format of the routing messages: route requests (RREQs), route replies (RREPs), and so on. The format of the RREQ message in the original AODV is shown in Table 1 [22]. In ETARP, the field "hop count" is replaced with "energy count." "Energy count" here implies the prediction of average transmission energy to successfully deliver a data packet from the originator node to the node handling the request. The predictions are defined in (1)–(5) later in this section.

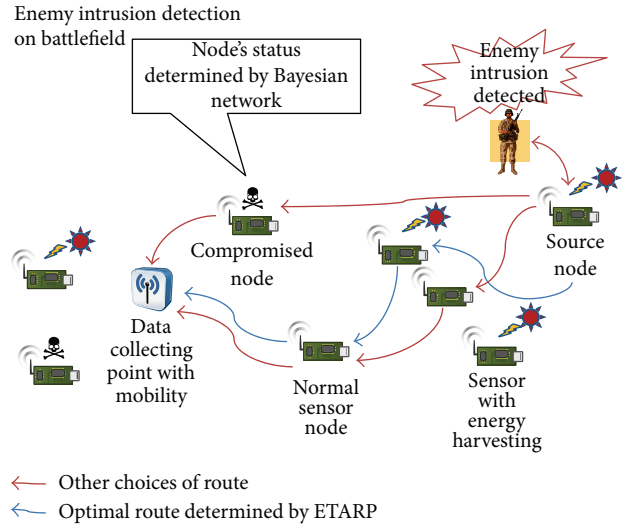

Figure 1: Example of WSN application scenario.

Table 1: RREQ message format in original AODV.

Type	R	A	Reserved	Prefix Sz	Hop count
Destination IP address					
Destination sequence number					
Originator IP address					
Lifetime					

The same change applies to the RREP message as well. The field "hop count" in the original AODV RREP message is replaced with "energy count" in the ETARP RREP message. Again "energy count" refers to the predicted average transmission cost to successfully deliver a data packet from the originator node to the destination node.

Since ETARP uses the same basic messages (RREQ, RREP, etc.) as AODV, it does not incur more overhead compared to the original AODV. The next question is how to define energy consumption.

On any chosen ith route with total number of j_i nodes, the expected total transmission cost E_i in terms of energy can be calculated as

$$E_i = E_{i1} + E_{i2} + \cdots + E_{i(j_i-1)}, \quad (1)$$

where E_{im} is the estimated transmission cost from the mth node on this route to its next hop ($1 \le m \le j_i - 1$).

Transmission cost depends on successful delivery of a packet possibly after a number of reattempts. To be more specific, transmission cost has the form

$$E_{im} = K_{im}\left(P_{im} + P_c + P_r\right)T, \quad (2)$$

where K_{im} is the predicted average number of retries after a packet is successfully transmitted from node m to its next hop node $m + 1$; P_{im} is the minimum required radio transmission power level at node m to successfully deliver a data packet to

the next hop; P_c is the processing power at node m (consumed by circuits for the preparation of radio transmission including coding and modulation); P_r is the receiving power at next hop $m+1$ (consumed for receiving data including demodulation and decoding); and T is the transmission time needed for each transmission attempt.

At least some of the nodes are assumed to be capable of harvesting solar energy. The harvested energy is considered free and accounted in E_{im} as

$$E_{im} = K_{im}\left(P_{im} + P_c + P_r - \alpha_{im}R\right)T, \tag{3}$$

where R is the maximum output power of the photovoltaic power generator and α_{im} is a random number in the range $[0, 1]$ if node m is capable of energy harvesting or $\alpha_{im} = 0$ if node m is not capable of energy harvesting. As mentioned in Section 1, solar cells are more suitable to be mounted on sensor nodes considering the size (e.g., wind driven generator is too bulky) or energy source accessibility (e.g., motion power is hard to access since nodes operate in severe environment where human activity is rare).

For nodes with energy harvesting, $\alpha_{im} = R'/R$ where R' is the active power level of the photovoltaic power generator. For a photovoltaic power generator [23], its active power is assumed to follow a β-distribution given by the probability density function:

$$F\left(R'\right) = \frac{\Gamma\left(p+q\right)}{\Gamma\left(p\right)\Gamma\left(q\right)}\left(\frac{R'}{R}\right)^{p-1}\left(1-\frac{R'}{R}\right)^{q-1}, \tag{4}$$

where p and q are the shape parameters of the distribution and Γ is the gamma function. Beta distributions are fit to the past record of sunlight data using the algorithm that minimizes the KS statistic [24], and its shape parameters p and q depend on the specific geographic location where sunlight data are recorded. This assumption is also based on the past recorded sunlight data and statistical correlation analysis of solar radiance and consumer load.

In order to successfully transmit a packet from node m to the next node, the expected average number of retries K_{im} can be calculated as

$$K_{im} = \frac{1}{1-e_{im}}, \tag{5}$$

where e_{im} is the probability of the packet not being delivered (or outage probability) from node m to node $m+1$ on any attempt [25]. Previous studies have shown that e_{im} can be expressed as a function of P_{im} [26].

After ETARP discovers a number of possible routes, say with energy costs $\{E_1, E_2, \ldots, E_N\}$, it selects the route with the minimum energy cost.

3.2. Energy Efficient and Secure Routing in Presence of Attacks. The previous section dealt with the simple case of energy efficient routing assuming normal conditions without attacks on the network. The possibility of attacks adds complications because nodes can become compromised and interfere with packet forwarding.

Our approach to add security awareness into ETARP relies on the concept of "expected utility" from utility theory. Either transmission energy or risk of untrusted nodes will diminish the expected utility of a route. ETARP seeks routes with high expected utility which will be both energy efficient and trusted.

In practical operation, ETARP requires changes in the format of control messages described earlier in Section 3.1. For instance, the "energy count" field in RREQ messages is replaced with "expected utility count" which here means the expected utility of the route from the originator node to the node handling the request. Similarly for the RREP message, the field "energy count" is replaced with "expected utility count" where expected utility count refers to the expected utility of the route from the originator node to the destination node.

3.2.1. Definition of Utility. Utility is a quite general concept known from microeconomics. In economics, utility is used to reflect a level of satisfaction of consumers when they purchase goods from a market. Usually the difficulty is how to exactly measure utility. Modern definitions of utility intend it to qualitatively reflect "consumer preferences". The goal is not to determine the exact value of utility, which is problematic, but to determine whether a choice of a particular good or product has a higher utility compared to others [27].

In WSNs, the utility or preference designated for a route is related to both energy cost and security level (trustworthiness). Consider a specific route consisting of M nodes ($M-1$ hops). Considering only energy on any specific hop, say the mth hop, the utility function is inversely proportional to the predicted transmission cost on this hop. Less energy consumption means a longer lifetime that is more "preferable" for the sensor nodes and therefore a higher utility. Then the utility function of the mth hop, denoted by u_m, satisfies $u_m \propto 1/E_m$, where E_m is the estimation of transmission cost from the mth node on this route to its next hop ($1 \le m \le M-1$).

The transmission on each hop takes place successively over time, starting from the source node and ending at the destination node. The utility of all these hops is imperfect substitutes to each other, meaning that some reduction in utility of mth hop might be compensated for to some extent by the addition in another hop's utility and vice versa. But this is not always the case; for example, if the mth hop is a dead link, no matter how good condition the other hops are, this route is considered to be useless with zero total utility. Due to this imperfect substitutes property, the utility function of a specific route belongs to the Cobb-Douglas type with standard form of $U = x^{\alpha}y^{\beta}z^{\gamma}\cdots\cdots$, where $x^{\alpha}, y^{\beta}, z^{\gamma}, \ldots\ldots$ denote the utility generated from first, second, third, $\ldots\ldots$ until the last ($M-1$th) hop on a route, respectively. That is, the utility of a route is the product of utility on all the $M-1$ hops [27]. On the other hand, wireless sensors deployed in a specific network typically belong to the same type with identical technical specifications; thus the sender nodes at each hop can be considered to be identical and use the same utility function to describe their "preference." In this case,

the multiple $M-1$ hops transmission on this route can be considered equivalent to a node repeating a single hop transmission $M-1$ times. Then the total utility on this route can be written as

$$U_{\text{route}} = \prod_{m=1}^{M-1} u_m = \prod_{m=1}^{M-1} \left(\frac{1}{E_m}\right)^c, \tag{6}$$

where c is a positive constant indicating the "preference" level of each hop, which is related to the sensitivity to energy cost.

Note that the numerator in the last part in (6) corresponds to the energy consumption factor on each hop, which is already explained in (3) of Section 3.1.

3.2.2. Calculation of Expected Utility. At each hop, there is a certain risk that the next node is compromised. In other words, there is never certainty about the status of any node (malicious or not). Given this uncertainty, we introduce the weighted average of utilities gained from all the possible results (malicious node or not) as the "expected utility" u'_m:

$$\begin{aligned} u'_m &= \left(S_m + (1-S_m)\,Q_m\right) u_m + (1-S_m)\,(1-Q_m)\,0 \\ &= \left(S_m + (1-S_m)\,Q_m\right) u_m, \end{aligned} \tag{7}$$

where S_m is the probability that the destination node is safe (not compromised) and Q_m is the possibility that the destination node is compromised but pretends to behave like normal node (a so-called "grey hole"). How to determine the probability S_m is explained in Section 3.3. If the node is safe or pretending to be normal, the utility of this hop is u_m. Otherwise the node is considered compromised with zero utilities. The total expected utility on the entire route is given by $U'_{\text{route}} = \prod_{m=1}^{M-1} u'_m$. As mentioned earlier, utility is only useful for acting as an indicator of preference between different choices of routes, and the precise utility value does not have any practical meaning.

ETARP discovers a number of possible routes, along with their expected total utility. It selects the route with the maximum total utility as the best route.

3.3. Estimation of Risk by Bayesian Network. Generally, it is difficult to ascertain whether a node has been actually compromised or not unless it is manifested in the node's observable behavior. A practical approach assumes that a risk can be estimated by observing the node's behavior compared to its expected behavior. In order to calculate a "belief" about a node's trustworthiness, a learning Bayesian network is proposed for this purpose. As addressed in Section 2, unlike the reputation management employed by previously proposed AOTDV or LTB-AODV which only watch a specific behavior, a Bayesian network is meant to organize the entire knowledge about observed node behavior into a coherent whole and makes comprehensive judgments on node status. Perhaps the use of joint probability distribution could be another approach to deal with multiple types of nodes behaviors, but the size of a joint probability distribution would be exponential in the number of nodes behaviors of interest, increasing both modeling and computational difficulties. On the other hand, a Bayesian network can address all of these difficulties in principle, by acting as a graphical modeling tool for specifying probability distributions [28].

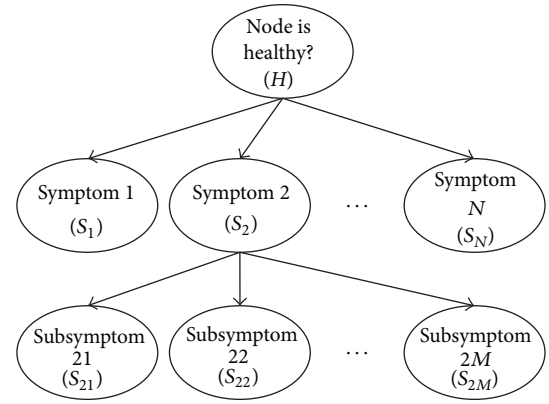

Figure 2: General Bayesian network structure.

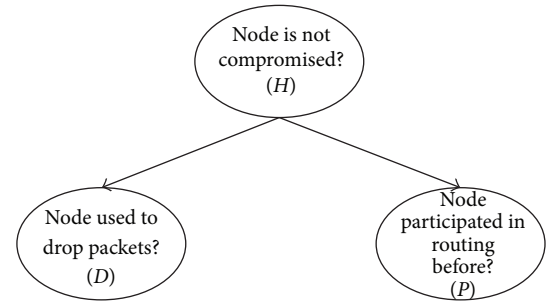

Figure 3: A Bayesian network example.

To be more specific, a Bayesian network is a probabilistic graphical model that represents a set of random variables and their conditional dependencies via a directed acyclic graph (DAG). Our Bayesian network serves to model a set of node status (comprised or not) and their behaviors. It can be used to predict the most likely status of a node based on past observed behaviors. To calculate this prediction, one method is the maximum likelihood approach.

A general Bayesian network structure employed in our case is shown in Figure 2. To determine whether a node is safe (not compromised, denoted by H), we need to observe the node's symptoms; some symptoms may require further observation on their subsymptoms.

Considering a basic practical example shown in Figure 3, the purpose is to determine a node's "health" status (node is compromised or not), denoted by variable H, two symptoms are considered: "node used to drop packets" (denoted by variable D). Note that it is normal for a node to drop packet sometimes for a valid reason, for example, bad link quality, but the term "drop packet" here implies that the number of dropped packets is unusually large. Also, "node participated in routing before or not" (denoted by variable P) can help to identify attacks including selective forwarding, sink hole, and black and gray hole. These variables are binary, represented by h_1 (true) or h_2 (false) for variable H, d_1 (true) or d_2

Table 2: Incomplete data sets $\mathscr{D}$.

$\mathscr{D}$	H	D	P
$\mathbf{case}_1$	?	d_2	p_1
$\mathbf{case}_2$	?	d_1	p_2
$\mathbf{case}_3$	?	d_1	p_1

(false) for D, and p_1 (true) or p_2 (false) for P. Circles in this DAG represent the aforementioned propositional variables. Edges in the graph represent "direct causal influences" among these variables; for example, the node participated in routing before (P) is a direct cause of node not being compromised (H). All these causal influences are presented by conditional probabilities, an example shown in the last two subtables of Table 3 (which is also an example of initial estimates to be explained later). Given this causal structure, one would expect the dynamics of changing belief to satisfy some properties. For example, if we get a record that the sensor node dropped a packet, our belief that the node participated in routing before would probably decrease.

In practical cases, the recorded node symptoms (referred to as data sets) are usually incomplete due to some reason; for example, a node is compromised or not cannot be directly observed (in fact, the purpose of creating Bayesian network is to determine it). Table 2 shows an example of incomplete data sets $\mathscr{D}$ with 3 different recorded data cases: $\mathbf{case}_1$, $\mathbf{case}_2$, and $\mathbf{case}_3$. A data case is a record of a set of symptoms shown by a node, in other words, a record with certain combination of instantiation (h, d, p), in which the status parameters h_1, d_1, and p_1 denote that this node has not been compromised, used to drop packet, and participated in routing before, respectively. And h_2, d_2, and p_2 denote that this node has been compromised, not used to drop packet, and not participated in routing before, respectively. The symbol "?" represents the missing values of variables.

The goal is to calculate the expected empirical distribution of nodes status H based on the incomplete data set. Some initial estimates are assumed as shown in Table 3 based on common sense; a comprised node is more likely to drop data packet and not participate in previous routing. On the other hand, a compromised node is more likely to participate in routing but may still drop data packet for some reason, for example, data transmission error.

The expected empirical distribution of the incomplete data set $\mathscr{D}$ is defined as

$$F_{\mathscr{D}}(a) \stackrel{\text{def}}{=} \frac{1}{N} \sum_{\mathbf{case}_i, \mathbf{c}_i = a} F(\mathbf{c}_i \mid \mathbf{case}_i), \tag{8}$$

where a is an event with certain combination of instantiation (h, d, p), N is the size of the data set, and $\mathbf{c}_i$ are variables with unrecorded values of case $\mathbf{case}_i$.

For example, the probability of an instantiation h_1, d_2, p_1 (which denotes the following: node is not compromised, node did not use to drop packet, and node participated in routing before) is given by

$$F_{\mathscr{D}}(h_1, d_2, p_1) = \frac{F(h_1 \mid \mathbf{case}_1)}{3}. \tag{9}$$

Table 3: Initial estimates.

(a)

H	$F_{\mathscr{D}}(h)$
h_1	0.8
h_2	0.2

(b)

H	D	$F_{\mathscr{D}}(d \mid h)$
h_1	d_1	0.1
h_1	d_2	0.9
h_2	d_1	0.8
h_2	d_2	0.2

(c)

H	D	$F_{\mathscr{D}}(p \mid h)$
h_1	p_1	0.5
h_1	p_2	0.5
h_2	p_1	0.25
h_2	p_2	0.75

Repeating this process can obtain the probability of all the other instantiations (h_i, d_i, p_i). Then the expectation maximization estimate of a node not being compromised is written as

$$F_{\mathscr{D}}(h_1) = \sum F_{\mathscr{D}}(h_1, d_i, p_i). \tag{10}$$

Other parameters such as $F_{\mathscr{D}}(d \mid h)$ and $F_{\mathscr{D}}(p \mid h)$ can be calculated by

$$F_{\mathscr{D}}(d_i \mid h_i) = \frac{\sum F_{\mathscr{D}}(h_i, d_i \mid d_i)}{\sum F_{\mathscr{D}}(h_i \mid d_i)},$$
$$F_{\mathscr{D}}(p_i \mid h_i) = \frac{\sum F_{\mathscr{D}}(h_i, p_i \mid d_i)}{\sum F_{\mathscr{D}}(h_i \mid d_i)}. \tag{11}$$

All the results derived from (8) and (11) based on incomplete data sets $\mathscr{D}$ constitute the $\mathscr{D}$ estimates that serves as the replacement of initial estimates shown in Table 3. If we continue to observe the network and fetch new incomplete data sets $\mathscr{D}_1, \mathscr{D}_2, \ldots, \mathscr{D}_m$, where m is a positive integer, as proved in Chapter 17 in [28], for any m, $\mathscr{D}_{m+1}$ estimates have a higher likelihood than that of $\mathscr{D}_m$ estimates. Thus all the above procedures can be repeated to update the $\mathscr{D}$ estimates to $\mathscr{D}_1$ estimates, $\mathscr{D}_2$ estimates, and so on, in order to get estimates with higher likelihood.

A potential problem of the aforementioned Bayesian network based risk determination method is that certain suspicious node's (or "target node") behaviors need to be monitored by its neighboring nodes (so called "watcher") while these nodes themselves might be malicious. Whether these "watchers" are reporting honestly becomes a new issue. How to acquire correct behavior information of the target node under the existence of some dishonest "watchers" is considered a classical agreement problem called Byzantine Generals' Problem. If l is the number of dishonest watchers involved in the monitoring process, it has been proved that

we can still obtain the correct information of target node if the total number of "watchers" satisfies $n \geq 3l + 1$ [29].

Applying this property to our case, assume that the entire WSN network has nodes deployment density of ρ nodes/m^2, the malicious fraction of the network is v, and size of neighboring area of target node is Am^2; it can be concluded that the accurate status of a target node can be obtained if the number of watchers n involved in monitoring the target node satisfies

$$n \geq 3v\rho A + 1, \tag{12}$$

where n is clearly an integer.

4. Performance Evaluation

In this section, the safety performance and energy efficiency performance of the ETARP routing protocol are analyzed. Two competitors are chosen for comparison. The first protocol is LTB-AODV, which is dedicated to the mitigation of network attacks based on the observed past behaviors of nodes [19]. The other protocol for comparison is AODV-EHA which is an energy efficient protocol aware of energy harvesting [30].

In performance evaluation, "safety performance" involves the average number of compromised nodes that are likely to be encountered in a single transmission, given a specific malicious ratio. Likewise "energy efficiency performance" here involves the estimated energy cost after successfully delivering a data packet in a single transmission along the route discovered by a specific routing protocol.

4.1. Existing Protocols for Comparison

4.1.1. Overview of LTB-AODV to Compare Safety. In LTB-AODV [19], different "trust values" are computed for all the routes to represent the risk level; then the algorithm chooses the route with the least hops among the candidates having a trust value higher than a given threshold. Let $T_i^R(j)$ denote the level of trust of any specified node i on any chosen neighbor node j. It is calculated as

$$T_i^R(j) = \frac{\text{Number of packets forwarded by } j}{\text{Number of packets to be forwarded by } j}. \tag{13}$$

The values of the numerator and denominator are obtained by node i monitoring the traffic of its neighbor j.

For a complete route, the total trust value, denoted by T_{route}^R, is given as the product $T_{\text{route}}^R = \prod_{m=1}^{M-1} T_m^R$, where T_m^R is the trust value of the mth node on its next hop. LTB-AODV is a modification of the AODV protocol incorporating the above trust estimation technique. Thus LTB-AODV chooses the most trusted route.

4.1.2. Overview of AODV-EHA to Compare Energy Efficiency. In AODV-EHA [30], the predictions of data transmission cost (in terms of energy) are computed for all the routes while considering the energy harvesting technology. The algorithm chooses the route with the least energy cost approximation for data transmission. Let $E_i(j)$ denote the approximation of energy cost after a data packet is successfully delivered from any specified node i to any chosen neighbor node j; then, for a complete route, the total trust energy cost denoted by E_{route} is given as the sum $E_{\text{route}} = \sum_{m=1}^{M-1} E_m$, where E_m is the estimation of energy cost after successfully delivering a data packet from the mth node to its next hop. AODV-EHA is a modification of the AODV protocol incorporating the above energy cost estimation. Thus AODV-EHA chooses the most energy efficient route.

Table 4: Simulation parameters.

Parameters	Descriptions
Simulation Area	500 m × 500 m
Node radio range	250 m
Traffic type	CBR
Packet size	127 bytes
Data rate	20 kbps
Signal to noise ratio (SNR) Threshold β	10
Processing power level P_c	10^{-4} W
Receiving power level P_r	5×10^{-5} W
Outage requirement e_{im}^*	10^{-4}

4.2. Simulation Setup. The experimental evaluation is carried out by means of MATLAB simulations using the Monte-Carlo method. The two criteria considered are safety performance and energy efficiency performance.

The size of the simulated area is 500 m × 500 m. The communication range of each node is 250 m. Considering the WSN applications, this paper focuses on (as addressed in the beginning of Section 1) IEEE 802.15.4 which was chosen for the physical and data-link layer, which is suitable for low data rate but very long battery life applications [31]. According to the specification mentioned in [31], the traffic type is constant bit rate (CBR) with a data rate of 20 Kbps, and the size of each packet is 127 bytes. Since the transmission cost prediction partly depends on previous works [26]; therefore, for those parameters required for the prediction process, we continue to use same values as adopted in [26]. Details are listed in Table 4.

Every simulation contains a certain malicious fraction of the network. These compromised nodes are located randomly in the simulation area, and they are assigned with certain behaviors that can further affect the route discovery process.

4.3. Experimental Results. The chosen scenario is analogous to the application of enemy detection on the battlefield. The data collection device (possibly a human) could be assigned to any position in the area where the WSN is deployed, rather than being tied to a fixed place. The number of nodes in the simulated area varies from 50 to 90.

4.3.1. Safety Performance. Figure 4 shows the safety performance of the 3 protocols under different compromised ratios (10%–30%). It can be seen that, as the malicious ratio

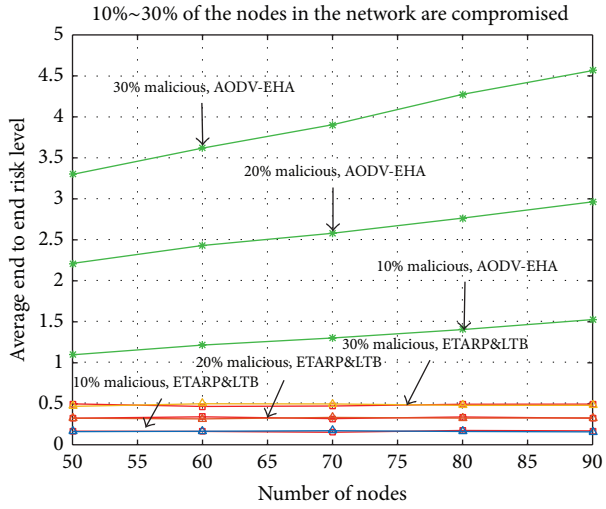

Figure 4: Average route risk level (average number of compromised nodes encountered on the route).

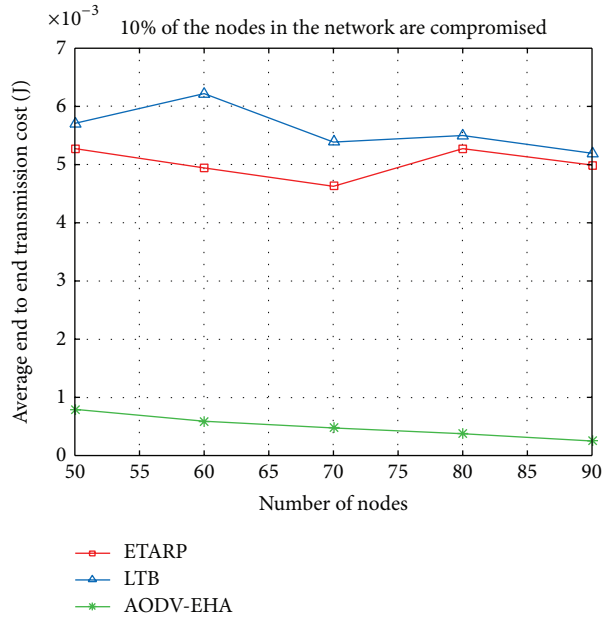

Figure 5: Average end to end transmission cost (Joule).

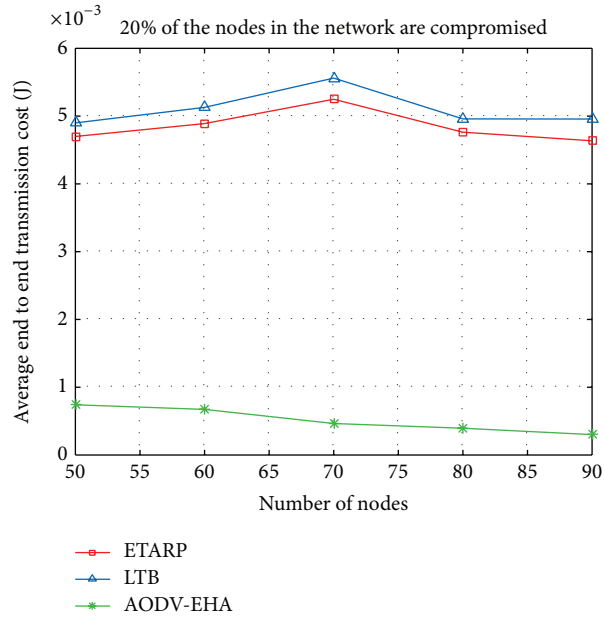

Figure 6: Average end to end transmission cost (Joule).

increases from 10% to 30%, the difficulty of maintaining security in the network is increasing. On the other hand, under different malicious ratios, the risk level lines of ETARP and LTB-AODV wind around each other while fluctuating a little bit as the nodes number increases. Therefore we can conclude that ETARP can maintain a similar safety performance as LTB-AODV.

By comparison, there is a more notable increment of risk level for AODV-EHA, as the malicious ratio increases in the network. Under any certain malicious ratio, the risk level line for AODV-EHA keeps increasing with the number of nodes in the network. This is due to the network coverage area remaining the same while the number of compromised nodes increases. Thus we can conclude that there is no security in AODV-EHA, as expected, since its original design did not take safety into consideration.

4.3.2. Energy Efficiency Performance. Figures 5–7 show the average energy cost of each transmission under different compromised ratios (10%–30%).

For any certain malicious ratio, both lines of ETARP and LTB-AODV fluctuate per number of nodes in the network. ETARP consistently uses less average transmission cost compared to LTB-AODV in terms of energy. More specifically, the energy cost of ETARP is reduced by 2.4% to 20.5% in comparison to that of LTB-AODV, depending on various situations.

On the other hand, the average transmission cost of AODV-EHA under any certain malicious ratio tends to decrease as the nodes number increases. The cost appears to be less than that of ETARP or LTB-AODV; but as illustrated in Section 4.3.1, the route determined by AODV-EHA is likely to be a dead-link almost in every transmission. A dead-link makes the theoretical minimum energy cost of AODV-EHA meaningless, since the packets are probably dropped on their way without reaching destination. All the energy already spent on the transmission is wasted, even though it is ostensibly less than that of ETARP.

From all the above results gained from safety and energy efficiency performance evaluations, we can conclude that, under different compromised ratios, ETARP has advantages in terms of energy efficiency in transmission while it can still maintain almost the same safety performance as LTB-AODV at the same time (stated in Section 4.3.1). By comparison, even though AODV-EHA achieves the theoretical "lowest" transmission cost, there is no security in AODV-EHA since

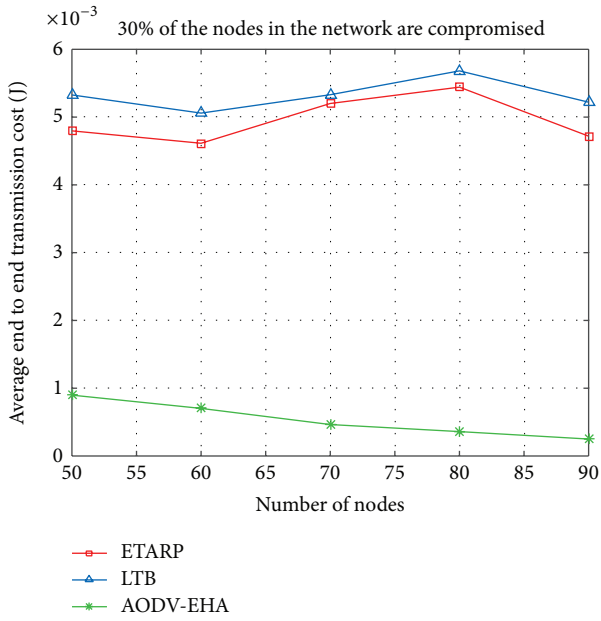

Figure 7: Average end to end transmission cost (Joule).

its original design focused on reducing energy cost but did not give attention to security.

A large network can be considered an interconnection of many smaller ones. We believe that the current results can be generalized to larger networks for the following reasons.

Suppose we are trying to find an optimal route from a specific source to a specific destination in a large network. The whole optimal route could be further decomposed to multiple subroutes; each one traverses a smaller subnetwork. Since these subnetworks are part of the whole network, they shall keep some identical properties, for example, nodes density and malicious rate. Therefore, for the same routing protocol, the subroute of the whole optimal route also serves as the optimal route in the corresponding subnetwork. In other words, for the same routing protocol, its routing process in the whole network is equivalent to the repeat of routing process in multiple subnetworks, and this protocol will not show a different and surprising behavior in a large network compared to the behavior of smaller ones.

Figure 8 shows a simple example of the aforementioned network decomposition; the whole optimal route is divided into 2 subroutes and transverses 2 subnetworks. The number of subroutes and subnetworks could be extended to any volume.

5. Conclusions

In this paper, we introduced the ETARP routing protocol for WSN applications operating in extreme environments usually for military use, such as SDT and ASW. ETARP simultaneously considers energy efficiency and security concerns by taking advantage of utility theory. Through simulations, we evaluated the energy efficiency performance and safety performance of ETARP in comparison to LTB-AODV and

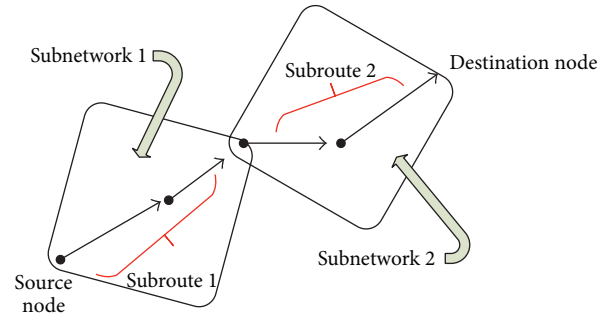

Figure 8: Example of network decomposition.

AODV-EHA. Results show that although AODV-EHA has the theoretical "lowest" transmission cost, there is no security in it, while ETARP has the advantages in terms of energy efficiency in transmission while it can still maintain the same safety performance as LTB-AODV.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] S.-H. Yang, *Wireless Sensor Networks: Principles, Design and Applications*, Springer, London, UK, 2014.

[2] P. Naz, S. Hengy, and P. Hamery, "Soldier detection using unattended acoustic and seismic sensors," in *Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR III, 83890T*, vol. 8389 of *Proceedings of SPIE*, Baltimore, Md, USA, April 2012.

[3] J. P. Towle, D. Herold, R. Johnson, and H. Vincent, "Low cost acoustic sensors for littoral anti-submarine warfare (ASW)," in *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense VI*, vol. 6538 of *Proceedings of SPIE*, Orlando, Fla, USA, April 2007.

[4] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, May 2003.

[5] E. M. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Personal Communications*, vol. 6, no. 2, pp. 46–55, 1999.

[6] V. Rodoplu and T. H. Meng, "Minimum energy mobile wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1333–1344, 1999.

[7] J.-H. Chang and L. Tassiulas, "Energy conserving routing in wireless ad-hoc networks," in *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '00)*, vol. 1, pp. 22–31, IEEE, March 2000.

[8] F. Ye, A. Chen, S. Lu, and L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks," in *Proceedings of the 10th International Conference on Computer Communications and Networks*, pp. 304–309, Scottsdale, Ariz, USA, October 2010.

[9] S. Chalasani and J. M. Conrad, "A survey of energy harvesting sources for embedded systems," in *Proceedings of the IEEE Southeastcon*, pp. 442–447, Huntsville, Ala, USA, April 2008.

[10] M. K. Jakobsen, J. Madsen, and M. R. Hansen, "DEHAR: a distributed energy harvesting aware routing algorithm for ad-hoc multi-hop wireless sensor networks," in *Proceedings of the IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM '10)*, pp. 1–9, Montreal, Canada, June 2010.

[11] S. S. Beheshtiha, H.-P. Tan, and M. Sabaei, "Opportunistic routing with Adaptive Harvesting-aware Duty Cycling in energy harvesting WSN," in *Proceedings of the 15th International Symposium on Wireless Personal Multimedia Communications (WPMC '12)*, pp. 90–94, Taipei, Taiwan, September 2012.

[12] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.

[13] F. Stajano and R. Anderson, "The resurrecting duckling: security issues for ubiquitous computing," *Computer*, vol. 35, no. 4, pp. 22–26, 2002.

[14] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04)*, pp. 162–175, ACM, New York, NY, U, November 2004.

[15] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[16] R. Watro, D. Kong, S.-F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: securing sensor networks with public key technology," in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)*, pp. 59–64, ACM, New York, NY, USA, October 2004.

[17] A. Liu and P. Ning, "TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks," in *Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN '08)*, pp. 245–256, April 2008.

[18] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, "Trust-based on-demand multipath routing in mobile ad hoc networks," *IET Information Security*, vol. 4, no. 4, pp. 212–232, 2010.

[19] N. Marchang and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks," *IET Information Security*, vol. 6, no. 2, pp. 77–83, 2012.

[20] H.-W. Ferng and D. Rachmarini, "A secure routing protocol for wireless sensor networks with consideration of energy efficiency," in *Proceedings of the IEEE Network Operations and Management Symposium (NOMS '12)*, pp. 105–112, Maui, Hawaii, USA, April 2012.

[21] M. Alshowkan, K. Elleithy, and H. Alhassan, "LS-LEACH: a new secure and energy efficient routing protocol for wireless sensor networks," in *Proceedings of the 17th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications (DS-RT '13)*, pp. 215–220, Delft, Netherlands, October 2013.

[22] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," RFC 3561, 2003.

[23] S. H. Karaki, R. B. Chedid, and R. Ramadan, "Probabilistic performance assessment of autonomous solar-wind energy conversion systems," *IEEE Transactions on Energy Conversion*, vol. 14, no. 3, pp. 766–772, 1999.

[24] R. D. Collins and K. G. Crowther, "Systems-based modeling of generation variability under alternate geographic configurations of photovoltaic (PV) installations in Virginia," *Energy Policy*, vol. 39, no. 10, pp. 6262–6270, 2011.

[25] J. H. Kleinschmidt, W. C. Borelli, and M. E. Pellenz, "An analytical model for energy efficiency of error control schemes in sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '07)*, pp. 3895–3900, June 2007.

[26] A. K. Sadek, W. Yu, and K. J. R. Liu, "On the energy efficiency of cooperative communications in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 6, no. 1, article 5, 2009.

[27] H. Varian, *Intermediate Microeconomics: A Modern Approach*, W W Norton & Company Incorporated, 2010.

[28] P. A. Darwiche, *Modeling and Reasoning with Bayesian Networks*, Cambridge University Press, New York, NY, USA, 1st edition, 2009.

[29] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[30] P. Gong, Q. Xu, and T. M. Chen, "Energy harvesting aware routing protocol for wireless sensor networks," in *Proceedings of the 9th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP '14)*, pp. 171–176, Manchester, UK, July 2014.

[31] "IEEE standard for local and metropolitan area networks part 15.4: low-rate wireless personal area networks (lrwpans) amendment 5," IEEE P802.15.4k/D5, 2013.